**IT Applications Unit 3, AOS 1, Online Communities**

**Complete the following, from pgs, 32: Network security**

**NETWORK SECURITY**

1. **What types of physical security measures can be put in place?**

Physical security measures such as locks and alarms are used to warm off intruders.

**Usernames and passwords**

1. **Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.**

* Include non alphabetical characters.

**Firewall**

1. **Describe the nature of a firewall.**

A firewall is a server and software combination that filters the information coming through the internet connection into an organisation’s internal network.

1. **What are the main purposes of firewalls and how are these purposes achieved?**

The main purposes of a firewall are to:

* Examining the IP address of computers that request information from an internal server
* Blocking all access to domain names
* Banning certain protocols from accessing certain servers
* Blocking certain words and phrases included in packets of information.
* Used to restrict employees’ access to certain information.

1. **Why do firewalls use 2 separate NICs?**

Firewalls use two separate NIC cards to determine whether the information is coming from the internal network or externally. The firewalls know if the information has come from outside the network because it won’t be identified as coming from the device with that common NIC. When outside access I requested the packets of information are immediately considered dangerous.

**Malware protection**

1. **What is malware and what strategies are used to protect against this type of software?**

Malware refers to malicious software and it includes spyware, adware, Trojan horses, worms and viruses. Computers should have anti-virus software installed and regularly updated for protection from malware.

**Encryption**

1. **What is encryption?**

Encryption is the process of translating data into a secret code that can only be read by authorised users. To read the encrypted file you must have a secret key that you use to decrypt the data.

1. **Describe the nature of WPA or WPA2.**

Wi-Fi protected access is a security protocol for use by wireless LANs. It provides security by encrypting data sent over radio waves so that it is protected during transmission from the sending device to the receiving device. WPA is designed to provide the same level of security to the wireless environment as a wire network would.

1. **What is encrypted data known as?**

Encrypted data is known as cipher text and unencrypted data is known as plain text.

**Secure Websites**

1. **Describe the secure protocol to allow secure financial transactions across the internet.**

The transactions are encrypted and authenticated as they travel across the internet by industry standard 128-bit SSL encryption to protect the privacy of the information.

1. **What is digital identification certificate technology based on?**

Digital identification certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

1. **Describe the nature of Secure sockets layer (SSL) protocol.**

Secure sockets layer is a cryptographic protocol that provides secure connection to the internet.

**Physical design of networks**

1. **What is the role of a network diagram?**

A network diagram is schematic method of showing the physical devices and communication lines present in a network. The diagrams use straight lines to represent cables and icons are used for communication devices.